Q4 2021 Privacy & Data Protection Report

As previewed in the EOY Information Security Board Report, this report provides focus on our top Information Security Risks.

2021 Top Risks Review

Access Control & Exceptional Access to Production Environments

Twitter has a large number of employees with direct access to our production environment. Every Engineer joining the company is provided Production level access. For context about half of all FTE employees[1] are engineers. Best practices are for companies to only allow production access to engineers in very minimal amounts and only in extreme situations (temporarily). Development, test, and staging environments are where engineers should safely conduct the majority of their work. We do not (meaningfully) have such environments. Twitter performs nearly all of these functions directly in production--thus requiring engineers to have production access. Further to this broad access to production, there are several pockets of exceptional access risk[2]. All of this is a-typical for security mature companies due to the risk associated with providing direct access to live customer data and the systems providing the service.

7714 FTEs

Strong access management to the various data and systems throughout Twitter's entire organization is the cornerstone to not only security and privacy but to enabling people to develop with velocity. To be explicit, access control is the primary line of defense to protect against a variety of threats (i.e., internal bad actors[3], misuse of data for otherwise legitimate business purposes as occurred in SIM-28--*which were the root cause of the current FTC issues*--accidental data spills, etc.).

CHART HERE

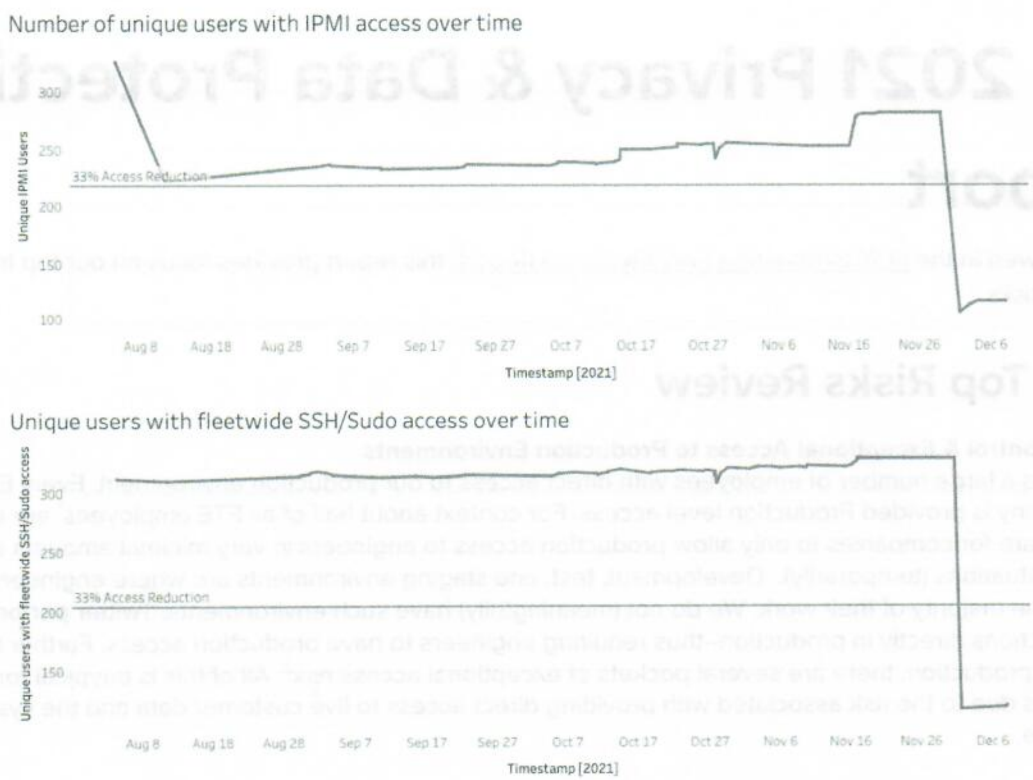
While needed progress has not been made on the larger issue of production access and access to production data (charts above) there have been reductions in two smaller groups of specifically troublesome access rights: IPMI and fleetwide "god" mode access.

[1] *Twitter was just shy of 8,000 FTEs as of November 30,2021, with ~4,000 engineers. A random security issue with an employee or their account would yield credentials that could access production data on average 50% of the time.*

[2] *320 people have superuser access across all systems and data within production and 250+ can remotely disable ("turn off") hardware within data centers.*

[3] See the statistics in the #Protect presentation

Extraordinary Access summary metrics over time



○

These groups need to be essentially eliminated (there should be less than 1-5% of employees with these permissions) as they provide unfettered access across all systems within our data centers and all service data and processes. Initial access reductions in these two

12-28-2020: SSH 2765(46.7%), Hadoop 2855(48.2%), MESOS 2442(41.3%), (FTE: 5917)
4-20-2021: SSH 3133(48.1%), Hadoop 3086(47.4%), MESOS 2778(42.7%), (FTE:6507)
12-13-2021: SSH 3399(51.8%), Hadoop 3679(47.7%), MESOS 3534(45.8%), (FTE: 7714)

Security Management of Systems and Software
Our next top risk we must report to the Board is the state of our security configuration and compliance across our client fleet (laptops and workstations) and servers. We have ~9,000 laptops in our fleet. It had been internally reported that all (about 99%) of our clients correctly have security monitoring software installed on them. Unfortunately this hid the critical aspect of what the security monitoring software was reporting. It has been revealed that more than half (58%) of our entire laptop fleet is out of security compliance, and one-third (33%) do not have software and security updates enabled on them.

12/13 graph